Technisch-Organisatorische Maßnahmen nach Art. 32 DSGVO

Name: _____

Organisation: _____

Adresse: _____

Inhalt

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 2
a) Zutrittskontrolle 2
b) Zugangskontrolle 2
c) Zugriffskontrolle 3
d) Trennungskontrolle 3
e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) 3
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO) 4
a) Weitergabekontrolle 4
b) Eingabekontrolle 4
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) 4
a) Verfügbarkeitskontrolle 4
b) Wiederherstellbarkeitskontrolle (Art. 32 Abs. 1 lit. c DSGVO) 5
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) 5
a) Datenschutz-Management 5
b) Incident-Response-Management 5
c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) 6
d) Auftragskontrolle 6

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungs-anlagen haben:

- ☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ☐ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- ☐ Sicherheitstüren / -fenster
- ☐ Gitter vor Fenstern/Türen
- ☐ Zaunanlagen
- ☐ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☐ Werkschutz, Pförtner
- ☐ Alarmanlage
- ☐ Videoüberwachung
- ☐ Spezielle Schutzvorkehrungen des Serverraums
- ☐ Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und/oder sonstigen Datenträgern
- ☐ Nicht-reversible Vernichtung von Datenträgern
- ☐ Mitarbeiter- und Berechtigungsausweise
- ☐ Sperrbereiche
- ☐ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
- ☐ sonstiges:

b) Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- ☐ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☐ Autorisierungsprozess für Zugangsberechtigungen
- ☐ Begrenzung der befugten Benutzer
- ☐ Single Sign-On
- ☐ BIOS-Passwörter
- ☐ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- ☐ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- ☐ Personalisierte Chipkarten, Token, PIN-/TAN, etc.
- ☐ Protokollierung des Zugangs
- ☐ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☐ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☐ Firewall
- ☐ sonstiges:

c) Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- ☐ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☐ Abschluss von Verträgen zur Auftragsdatenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von pbD, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.
- ☐ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☐ Autorisierungsprozess für Berechtigungen
- ☐ Genehmigungsroutinen
- ☐ Profile/Rollen
- ☐ Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, VeraCrypt, Safe Guard Easy, Zip-Programm, PGP)
- ☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. durch Kopierschutz, Sperrung von USB-Ports, „Data Loss Prevention (DLP)-System“)
- ☐ „Mobile Device Management-System“
- ☐ Vier-Augen-Prinzip
- ☐ Funktionstrennung „Segregation of Duties“
- ☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- ☐ Nicht-reversible Löschung von Datenträgern
- ☐ Sichtschutzfolien für mobile Datenverarbeitungssysteme
- ☐ sonstiges:

d) Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- ☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken
- ☐ Verarbeitung auf getrennten Systemen
- ☐ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ☐ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ☐ Mandantenfähigkeit von IT-Systemen
- ☐ Verwendung von Testdaten
- ☐ Trennung von Entwicklungs- und Produktionsumgebung
- ☐ sonstiges:

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten stellen in einer Weise sicher, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;:

- ☐ Durchführen von Pseudonymisierungs-Maßnahmen

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- ☐ Verschlüsselung von Email bzw.- Email-Anhängen (z.B. Zip-Programm)
- ☐ Verschlüsselung des Speichermediums von Laptops
- ☐ Gesicherter File Transfer (z.B. sftp)
- ☐ Gesicherter Datentransport (z.B. SSL, ftp, ftps, TLS)
- ☐ Verschlüsselung von CD/DVD- ROM, externen Festplatten oder USB-Sticks (z.B. VeraCrypt, Safe Guard Easy, PGP)
- ☐ Physikalische Transportsicherung
- ☐ Verpackungs- und Versandvorschriften
- ☐ Elektronische Signatur
- ☐ Gesichertes WLAN (mindestens WPA2)
- ☐ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- ☐ „Mobile Device Management-System“
- ☐ „Data Loss Prevention (DLP)-System“
- ☐ Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- ☐ Protokollierung von Datenübertragung oder Datentransport
- ☐ Protokollierung von lesenden Zugriffen
- ☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- ☐ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)
- ☐ sonstiges:

b) Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- ☐ Zugriffsrechte
- ☐ Systemseitige Protokollierungen
- ☐ Dokumenten Management System (DMS) mit Änderungshistorie
- ☐ Sicherheits-/Protokollierungssoftware
- ☐ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☐ Mehraugenprinzip
- ☐ „Data Loss Prevention (DLP)-System“
- ☐ sonstiges:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Verfügbarkeitskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- ☐ Sicherheitskonzept für Software- und IT-Anwendungen
- ☐ Backup Verfahren
- ☐ Aufbewahrungsprozess für Backups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☐ Gewährleistung der Datenspeicherung im gesicherten Netzwerk

- ☐ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☐ Spiegeln von Festplatten
- ☐ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☐ Geeignete Archivierungsräumlichkeiten für Papierdokumente
- ☐ Brand- und/oder Löschwasserschutz des Serverraums
- ☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- ☐ Klimatisierter Serverraum
- ☐ Virenschutz
- ☐ Firewall
- ☐ Sonstiges:

b) Wiederherstellbarkeitskontrolle (Art. 32 Abs. 1 lit. c DSGVO)

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nach zufälliger Zerstörung oder Verlust rasch wieder hergestellt werden können:

- ☐ Notfallplan
- ☐ Erfolgreiche Notfallübungen
- ☐ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
- ☐ sonstige:

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a) Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- ☐ Datenschutzleitbild
- ☐ Datenschutz-Richtlinie
- ☐ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- ☐ Bestellung eines Datenschutzbeauftragten
- ☐ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☐ Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- ☐ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- ☐ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- ☐ Ext. Prüfung/Auditierung der Informationssicherheit (etwa im Rahmen von ISO-Zertifizierung)
- ☐ sonstige:

b) Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- ☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- ☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- ☐ sonstige:

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die Default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt:

- ☐ Beispiele (z. B. Kennzeichnung von Eingabefeldern in Onlineformularen als Pflichtfelder, obwohl die Inhalte für die weitere Bearbeitung nicht notwendig sind.)

d) Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- ☐ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- ☐ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☐ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☐ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ☐ Unabhängige Auditierung der Weisungsgebundenheit
- ☐ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☐ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- ☐ formalisiertes Auftragsmanagement
- ☐ dokumentiertes Verfahren zur Auswahl des Dienstleisters
- ☐ standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister
- ☐ sonstiges:

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift
_____	_____
Name, Funktion Unterzeichner (in Druckbuchstaben)	Name, Funktion Unterzeichner (in Druckbuchstaben)

Mit freundlicher Empfehlung:

COMMPACT GmbH
Gesellschaft für Informationstechnologie
COMMPACT GmbH
Gesellschaft für Informationstechnologie
Adolph-Kolping-Str. 6
17034 Neubrandenburg
www.commpact.de
@-Mail: info@commpact.de
Tel.: 0395 56 86 0
Fax: 0395 56 86 150